IT Handbook Presentation
Audit Booklet

	Visual	Narrative
1.	**IT Handbook Presentations** **Audit** 	Open music
2.	**Changes** - Organization - Content 	Readers will find both organizational and content changes between the new Audit Booklet and the Internal/External Audit chapter of the 1996 IS Examination Handbook.
3.	**Changes** - Organization – Examiner perspective – Comprehensive action summaries	The booklet was reorganized to follow the actual flow of the examination process. Each section in the booklet now relates directly to a high-level issue that is of importance to examiners, and the booklet's action summaries provide a comprehensive synopsis of the content in each section.
4.	**Changes** - Organization - Content – Sarbanes-Oxley Act – Gramm-Leach-Bliley Act 	The new contents include changes in the examination process brought about by legislation that has been enacted since 1996 such as: ▪ The Sarbanes-Oxley Act of 2002, which addresses independence of board audit committees and accounting firms, and ▪ Section 501(b) of the Gramm-Leach-Bliley Act of 1999, which expanded security requirements for customer information.

	Visual	Narrative

5.	**Changes**
	- **Content**
	  – Sarbanes-Oxley Act
	  – Gramm-Leach-Bliley Act
	  – **Outsourcing of IT audits**
	  – **Third-Party reviews**
		In addition, the booklet specifically addresses two issues that have become of particular significance since 1996—outsourcing of IT audits and third-party reviews.

6.	**Outsourcing IT Audits** 	In recent years, more and more institutions have begun to outsource IT audits.
7.	**Outsourcing IT Audits** - **Cost savings** 	This increase is due, in part, to current business models that see outsourcing as a way to cut operating costs.
8.	**Outsourcing IT Audits** - **Cost savings** - **Increased specialization** 	IT in financial institutions has become increasingly prominent and complex over the past decade. It now requires a greater range and depth of IT audit skills to conduct effective internal audits, making it more and more expensive for an organization to maintain an adequate IT audit staff. The result of this trend is that a greater number of institutions are outsourcing some or all of their internal IT audit function in order to decrease overhead while maintaining or enhancing IT audit expertise.

	Visual	Narrative
9.	**Changes** ▪ **Content** – Sarbanes-Oxley Act – Gramm-Leach-Bliley Act – **Outsourcing of IT audits** – Third-Party reviews	In response to these changes, the Audit Booklet addresses IT audit outsourcing as a separate topic.
10.	**Third-Party Reviews** ▪ **Standards for external auditors** – **SAS 70** – **Trust services reviews**	New information on third-party reviews of technology service providers includes perspectives on standards for external auditors by the AICPA - the American Institute of Certified Public Accountants. These include: - SAS 70 or Statement on Auditing Standards Number 70 (a widely recognized standard indicating that a service provider has had its control objectives examined by an independent accounting firm). - Trust Services (advisory- and assurance-level engagements such as SysTrust® and WebTrust® conducted by independent auditors using a core set of principles, criteria, and illustrative controls).
11.	**Residual Content** ▪ **Structure** ▪ **Role, independence, and staffing** ▪ **Role of external audit** ▪ **Risk-based methodology** ▪ **Audit participation** 	There are also topics that remain substantially the same as they appeared in the earlier handbook. Key areas in a sound auditing program still include: ▪ The structure of an internal audit function, ▪ The role, independence, and staffing of internal IT Audit, ▪ The role of external audit ▪ Risk assessment and risk-based auditing methodology, and ▪ Audit participation in application acquisition, development, and testing.
12.	**Presentation** ▪ **Changes** – **Organization** – **Content** ▪ **Booklet organization**	Having considered some of the ways that the content in the booklet compares to that in the 1996 IS Examination Handbook, let's take a look at how the new booklet is organized.

	Visual	Narrative
13.	**Booklet Organization** ▪ IT Audit Roles and Responsibilities ▪ Independence and Staffing of Internal IT Audit ▪ Internal Audit Program	The first three sections address the basic requirements for implementing and staffing an effective internal audit program.
14.	**Booklet Organization** ▪ IT Audit Roles and Responsibilities – Board of directors and senior management – Audit management – Internal audit staff – Operating management – External auditors	First, the *IT Audit Roles and Responsibilities* section outlines audit program responsibilities for: ▪ The board of directors and senior management, ▪ Audit management, ▪ The internal audit staff, ▪ Operating management, and ▪ External auditors.
15.	**Booklet Organization** ▪ IT Audit Roles and Responsibilities ▪ Independence and Staffing of Internal IT Audit – Independent audit staff – Audit staff skills	The next section, *Independence and Staffing of Internal IT Audit*, covers the importance of the: ▪ Independence of audit staff from operations management, and ▪ Skill level requirements being commensurate with the scope and sophistication of the institution's IT environment.
16.	**Booklet Organization** ▪ IT Audit Roles and Responsibilities ▪ Independence and Staffing of Internal IT Audit ▪ Internal Audit Program	▪ Finally, the *Internal Audit Program* section outlines guidelines for developing and maintaining a formal internal audit program, including IT audits.

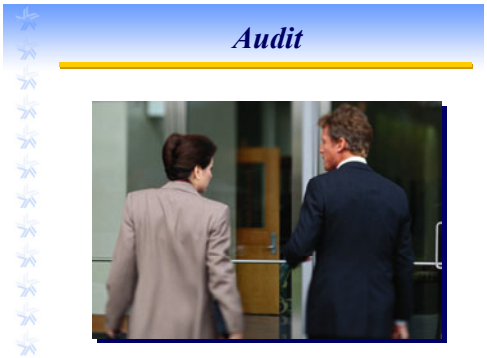
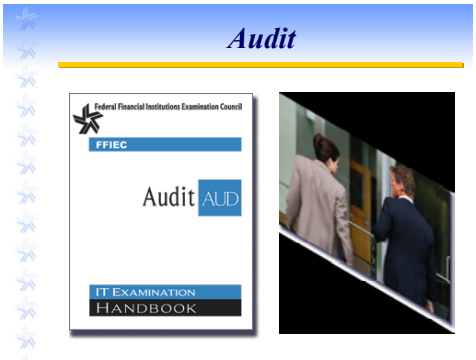
	Visual	Narrative
17.	**Booklet Organization** - Implementing and staffing sections - **Risk Assessment and Risk-Based Auditing**	While the three previous sections address the implementation and staffing of internal audit programs, the next section covers the nature of, and requirements for, a risk-based approach to auditing.
18.	**Risk-Based Approach** 	As with other IT Booklets, this booklet describes a risk-based approach to IT auditing, which includes performing an IT risk assessment and developing risk-based audit plans.

19.	**Risk-Based Approach**
	- **Risk-based assessment**
	  – **Identification**
	  – **Ranking**
	  – **Development**
	  – **Implementation**
		The booklet's guidelines for performing a risk assessment include:
		▪ Identifying institutional resources and business activities,
		▪ Ranking risks for significant business units and products, and
		▪ Developing and implementing risk-based audit plans.

20.	**Audit Plans** - **Audit cycle length** - **Documentation requirements** - **Guidelines for overriding assessments**	These audit plans should include: ▪ Maximum lengths of audit cycles for each level of risk within an institution, ▪ Specific documentation requirements, and ▪ Guidelines for overriding risk assessment cycles when dictated by special circumstances.

	Visual	Narrative
21.	**Booklet Organization** - Implementing and staffing sections - Risk-Based approach - **Additional Topics**	The final three sections of the booklet take a look at additional topics related to the IT audit function, including:
22.	**Alternative Activities** - **Audit participation:** – **Application development** – **Acquisition** – **Conversions** – **Testing** - **Outsourcing Internal IT Audit** - **Third-Party Reviews of Technology Service Providers**	▪ *Audit participation in application development, acquisition, conversions and testing;* ▪ *Outsourcing internal IT audit; and* ▪ *Third-party reviews of technology service providers.*
23.	**Appendices** **A: Examination Procedures** **B: Glossary** **C: Laws, Regulations, and Guidance**	The booklet provides the standard IT Handbook appendices for: ▪ Examination Objectives and Procedures, ▪ Glossary, and ▪ Laws, Regulations, and Guidance.
24.	**Examination Procedures** - **Tier I** - **Tier II** 	The examination objectives and procedures take a two-tier approach. Tier I primarily follows the organization of the booklet, providing tools for a detailed review of the effectiveness of the institution's audit function to identify and manage risks.

	Visual	Narrative
25.	**Examination Procedures** - Tier I - Tier II 	Tier II corresponds to the rating areas in URSIT, the Uniform Rating System for Information Technology, and provides additional validation, as warranted by risk, to verify the effectiveness of an institution's audit program.
26.	**Examination Procedures** 	These two tiers of examination objectives and procedures provide a wide range of inquiries from which examiners can select specific issues significant for the particular institution they are examining.
27.	**Appendices** A: Examination Procedures B: Glossary C: Laws, Regulations, and Guidance	Readers should also note the large number of resources listed in the Laws, Regulations, and Guidance appendix of this particular booklet.
28.	**Resources** 	These items can serve as a valuable complement to booklet content, and all are available from the FFIEC IT Handbook InfoBase.

	Visual	Narrative
29.		A strong audit program is essential to an institution's safe and sound operation. It provides the framework for ensuring effective risk management practices, internal controls, and compliance with corporate policies. In every examination, determining the quality of an institution's IT audit functions is a fundamental step in evaluating other aspects of the institution.
30.		The Audit Booklet provides comprehensive guidance for assessing the soundness and effectiveness of an institution's IT audit function.